E-SAFETY POLICY

Why is internet use important?

The educational benefits of internet access far outweigh the possible risks, and good planning and management will ensure appropriate and effective pupil use. Whilst regulation and technological solutions are very important, their use must be balanced by teaching pupils to take a responsible approach, and this forms an essential part of the school's e-safety provision.

How will the internet provide effective learning?

The purpose of internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management of information and business administration systems. Internet access provides many high-quality teaching and learning resources, some free, some subscription, as well as providing huge potential for research.

How will internet access be authorised?

Internet access will be granted to a whole class or individuals as part of a scheme of work, after suitable education in responsible internet use. Older pupils may carry out their own internet searches for research purposes and should know how to conduct searches safely and what to do if they come across something unsuitable.

Pupils' entitlement to use the internet is based on their responsible use of it. Irresponsible use may result in this privilege being removed.

How will the school ensure internet access is as safe as is reasonably possible?

Levels of access and supervision will vary according to pupil's age and experience.

The school uses an internet filtering system that is designed to filter out material found to be inappropriate for use in the education environment. We also use anti-virus and firewall software that will perform this function more effectively. The systems we use are Sophos and Linksys. Additionally, children are taught to use the 'safe search' function on the home page of the school's website, or a suitable alternative.

If staff or pupils discover unsuitable sites, the URL address and content will be reported to the headteacher and logged in the 'ICT Reporting Record'. This will in turn be reported to the internet service provider.

The school will work in partnership with parents and internet providers to ensure systems to protect pupils are renewed and improved and are effective in practice.

How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material.

However, due to the international scale and linked nature of information available via the internet, it is not possible to guarantee that unsuitable material will never appear on a terminal. Methods to identify, access and minimise risks will be reviewed regularly by the teaching staff and school governors.

How will publishing on the web be managed?

The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' home information will NOT be published.

Photographs used on the website must not identity individual pupils by full name. Group shots will be used where possible and other carefully selected shots.

Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

Permission from parents/carers will be obtained when a pupil joins the school before photographs are published on the school website. Parents will be notified of their right to refuse to allow any pictures of their child to be shown.

Where audio and video are included, the nature of the items uploaded will not include content that allows the pupils to be identified.

Protecting personal data.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Personal data must be stored on a password-protected laptop or encrypted storage device (e.g. USB memory stick). All staff laptops are encrypted and the encryption status is checked every 6 months. A screen shot is taken and stored of the encryption check and stored as evidence. We have established an encrypted school server for the storage of photographs and limited pupil data and use Office 365 tools for e-mail, file sharing and secure cloud storage in order to comply with the new General Data Protection Regulation (GDPR) and New Data Protection Act (2018).

How will e-mail be managed?

Pupils may only use approved e-mail accounts on the school system. Whole class or group email addresses should be used at KS1 and monitored accounts at KS2, where incoming and outgoing messages are checked and authorised by the teacher before sending or receiving (thus all pupils' emails will be treated as 'public').

Pupils should use email in an acceptable way (being polite and considerate) and must immediately tell a teacher if they receive offensive or distressing messages.

Pupils must make sure they do not reveal any personal details about themselves or others in any online communication or arrange to meet anyone in person that they meet online.

Information will be provided to parents explaining how pupils can access their accounts from home.

Social networking and mobile phones.

Social networking sites, such as Facebook, Messenger, Instagram, WhatsApp and personal emailing etc are NOT allowed to be accessed by pupils or staff in school, with the exception of the official school sites.

Any digital communication between staff and pupils or parents (e.g. e-mail) should be professional in content.

As part of the school's e-safety education programme, pupils and parents will be advised that social networking sites are inappropriate for primary aged children. Pupils in KS2 will be taught about the potential risks and how to keep personal information safe. The purpose of this is to acknowledge (although not condoning) the reality that some children may already have access to social networking sites by this age.

Each year group will have specific ICT/PSHE lessons dedicated to e-safety.

Pupils are not permitted to bring mobile phones to school, unless, under exceptional circumstances, special permission has been granted by the headteacher. If permission is granted, the child's class teacher will collect them in for safekeeping at the start of the school day and return them at the end. Appropriate use of mobile phones will be taught to pupils as part of PSHE. Staff may use them only outside lessons, and out of sight of the children, unless contacting the school when on a trip/course.

How will staff and parents be informed about e-safety?

All staff will have access to this E-Safety Policy, and its importance explained with relevant training given.

The school will seek to draw attention to the school's E-safety Policy and provide information and awareness of key E-safety issues to parents/carers through newsletters and the school website.

How will pupils be informed about e-safety and evaluating content?

E-safety education will be provided in the following ways:

A planned E-safety programme should be provided as part of ICT/PSHE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technology in school and outside school.

Key E-safety messages should be reinforced as part of a planned programme of assemblies, including understanding the need for acceptable use, how to stay safe online and responsible use.

How will complaints be handled?

Responsibility for handling incidents will be given to the headteacher or delegated as the need arises.

Any complaint about staff misuse must be referred to the headteacher and then to the Chair of Governors. Any illegal apparent or actual misuse will be reported to the headteacher, or the police, as appropriate.

Complaints about misuse of the internet in school by pupils must follow the most relevant school's policy (i.e. Behaviour, Bullying, Racism, Health and Safety).

Cyber-bullying

See the school's separate policy on Counter Cyber-Bullying for advice and procedures on dealing with cyber-bullying.

Last date reviewed: October 2024

Next review date: October 2027